



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,332	12/02/2003	Wei Yen	57159-8009.US01	5294
22918	7590	07/09/2008		
PERKINS COIE LLP			EXAMINER	
P.O. BOX 1208			HOMAYOUNMEHR, FARID	
SEATTLE, WA 98111-1208				
			ART UNIT	PAPER NUMBER
			2139	
			MAIL DATE	DELIVERY MODE
			07/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/727,332

Applicant(s)

YEN ET AL.

Examiner

Farid Homayounmehr

Art Unit

2139

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 April 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21, 25-65, 69-84, 86, 87 and 89-97 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21, 25-65, 69-84, and 86, 87, 89-97 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is responsive to communications: application, filed 4/6/2001; amendment filed 4/7/2008.
2. Claims **1-21, 25-65, 69-84, and 86, 87, 89-97** are pending in the case.

Response to Arguments

3. Rejection under section 112 outlined in the last Office Action is withdrawn due to amendments by the applicant.
4. Applicant's argument is moot in view of the new grounds of rejection submitted in this action.

Information Disclosure Statement PTO-1449

Applicant submitted an Information Disclosure Statement on 5/29/2008, without submitting a form PTO-1449, listing the references. Therefore, no form PTO-1449 can be reviewed and submitted to the applicant.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Siann (US Patent Application No. 2003/0120541, filed 12/21/2001).

6.1. As per claim 1, Siann is directed to a method including providing a system including a playback device; generating a text-based activation code based on information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system (paragraph 39 describes access data as, for example, an authorization code, which is used to ensure that the media player can decrypt the content. Therefore, access data is used to permit execution of content (content being displayed) in the player device, which is the same as description of the activation code in applicant's specification page 15 lines 8-12. Paragraphs 97 and 98 clearly shows that access data is used to control access using cryptographic techniques which verify the data and allow access if the rules are satisfied. Paragraph 100 teaches configuring and providing (generating) the access data based on information specific to the certain media player);

sending to a device, via a transport technique not including in the playback device (Fig. 1B clearly indicates a transmission path separate from the media player, as described in paragraph 99. Note that the Media Player includes a play back device and a transmission/reception device and a device to enforce the access rules, and therefore the message is sent while not including the playback device. Also see paragraph 43, describing a method of transmission for transmitting the access data, which is separate from the method of transmission for the content), verifying the text-based activation code against the information obtained from the playback device (Fig. 1B and paragraph 43. Also parag. 80 shows access data allows rights information to be verified as it states: "Access data 164 allows the electronic media content 110 to be secure, such that the electronic media content 110 is usable only if the proper access data have been provided to the media player 120". As stated above, the access data is configured based on information specific to the player device. Therefore, the access data is verified against the information obtained form the play back device); enforcing the rights information on the system in response to the text-based activation code (paragraph 80 and 39).

6.2. As per claim 2, Siann is directed to a method as in claim 1, including steps of ensuring that only authorized content is executed or presented by the playback device or a secure processor, or by both in combination or conjunction (paragraph 98).

6.3. As per claim 3, Siann is directed to a method as in claim 1, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based activation code (Fig. 1B and associated text)

6.4. As per claim 4, Siann is directed to a method as in claim 1, wherein the steps of enforcing are performed at least in part by the playback device or a secure processor coupled thereto (paragraph 98).

6.5. As per claim 5, Siann is directed to a method as in claim 1, wherein the steps of enforcing are performed by mandatory security hardware or mandatory security software (paragraphs 53 and 96).

6.6. As per claim 6, Siann is directed to a method as in claim 1, wherein the steps of enforcing include steps of decrypting at least some information derivable from the text-based message (paragraph 43 discloses delivery of access data using text-based messages (SMS) and paragraph 105 discloses decrypting of access data using keys.).

6.7. As per claim 7, Siann is directed to a method as in claim 1, wherein the steps of enforcing includes using a key derived from the activation code for decrypting a license or content (paragraph 105).

6.8. As per claim 8, Siann is directed to a method as in claim 1, wherein the steps of enforcing includes putting together at least an identity of the playback device and an identity of content; applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content (paragraphs 105 and 106 describe content media access control based on messages directed to the Media Player. The system determines if the content should be played or not. Also, as stated in response to claim 1, the access data is configured based on the identity of the playback device. Therefore, the access is provided after the content and the playback device are identified and authenticated).

6.9. As per claim 9, Siann is directed to a method as in claim 1, wherein the steps of enforcing includes applying a key derived from the activation code as an authentication code (paragraph 56 discloses user and content identification data transmitted to media player as part of access data and paragraph 97 discloses securing access data using cryptographic methods).

6.10. As per claim 10, Siann is directed to a method as in claim 1, wherein the activation code is composed on an SMS (paragraph 43 teaches SMS as a method of transmission of the access code. Also see paragraph 57).

6.11. As per claim 11, Siann is directed to a method as in claim 1, wherein at least a portion of the activation code is manually entered into the playback device (paragraph 47 describes manual entry of the data by humans, which discloses manual entering of the access code to the media player by a human).

6.12. As per claim 12, Siann is directed to a method as in claim 1, wherein at least a portion of the activation code is provided to the playback device, wherein the playback device processes the portion of the activation code and produces a licensing message suitable to be sent by the device, and wherein the licensing message is provided to the device (paragraph 81. Also, paragraph 90 describes content provider payments when users play their content or download the licensed content. This clearly implies a licensing message from user to content providers via Media Player. Note that per paragraph 95 the communication between the Media Player and Content Providers is two way).

6.13 As per claim 13, Siann is directed to a method as in claim 12, wherein the licensing message is encrypted or cryptographically authenticated by the device and sent to a license server (per paragraphs 9 and 83, the communication between different elements is secured, and per paragraph 51, security is provided by use of cryptographic methods).

6.14. As per claim 14, Siann is directed to a method as in claim 1, wherein the steps of enforcing include steps of using a decryption key available to the playback device or a secure processor coupled thereto (paragraph 80).

6.15. As per claim 15, Siann is directed to a method as in claim 1, wherein said text-based activation code is included in a first message, further comprising sending a second message from the device to a license server (paragraph 81); sending a first message from the license server to the device (paragraph 81), the first message including human-readable characters; and manually entering those characters to an input element coupled to the playback device (paragraph 47 describes manual entry of the data by humans, which discloses manual entering of the access code to the media player by a human).

6.16. As per claim 16, Siann is directed to a method as in claim 1, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message (Fig. 1B and associated text).

6.17. As per claim 17, Siann is directed to a method as in claim 1, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor (paragraph 98).

6.18. As per claim 18, Siann is directed to a method as in claim 1, wherein the system includes a secure processor capable of authenticating content coupled to the playback device in response to that authentication code (Item 480 of Fig. 4 and associated text. Siann paragraph 79 discloses a header of media content that includes information to identify the content and access data. This data is used to authenticate the data and determine if the content should be made available to user).

6.19. As per claim 19, Siann is directed to a method as in claim 1, including steps of authenticating the right information by the playback device or a secure processor coupled thereto (right information is included in the access rules, paragraph 40. Siann's method provides access rules to the Media Player in a secured manner).

6.20. As per claim 20, Siann is directed to a method as in claim 1, further comprising decrypting at least some information derivable from the text-based activation code (paragraph 43 discloses delivery of access data using text-based messages (SMS) and paragraph 105 discloses decrypting of access data using keys).

6.21. As per claim 21, Siann is directed to a method as in claim 1, further comprising using a decryption key available to the playback device or a secure processor coupled thereto (paragraph 80).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 25-65, 69-84, and 86, 87, 89-97 are rejected under 35 U.S.C. 103(a) as being unpatentable over Siann (US Patent Application No. 2003/0120541, filed 12/21/2001).

7.1. As per claim 25, Siann is directed to a method comprising:
generating a text-based activation code of a sufficiently small size that is convenient for a human to enter based on information obtained from a playback device of a system (see response to claim 1, and note that Sian also teaches using SMS as a method to transmit the activation code (see claim 6 above). As SMS stands for Short Messaging System, the code is small enough to enter by human);
providing the text-based activation code via an SMS technique (see claim 6 above);
sending the text-based activation code in a text-based message to a hand-held device using an SMS technique, the text-based activation code including information from which rights information is verifiable by the system (see response to claim 1);
putting together, at the playback device, at least an identity of the playback device and an identity of content (see response to claim 8);

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content, wherein the text-based activation code is not used to authenticate the execution rights (see response to claim 8, and note that Siann also teaches access data can be sent to the player device in a separate channel from the media content.

According to paragraph 99 and 103, access rules and access data are transmitted in separate paths. Per paragraph 103, access rules may be programmed in the media player. Therefore, Siann teaches access rules (license) that is produced using data available in the play back device, and not using the access data (activation code). Also see parag. 68, where Siann teaches electronic media is Pre-loaded);

verifying the execution rights using at least part of the text-based activation code as a cryptographic signature (Siann parag. 98, in accordance with fig. 4, describes access rules, which provide information whether or not to allow media content to be used by the user. The access rules are used in combination with access data as a security mechanism to ensure that electronic content is secure. Therefore, Siann teaches a mechanism that in conjunction with access data, provides information sufficient for the secure player to verify the authenticity of the content and to use the content, and to verify that the specific user has rights to execute or present the content at the specific playback device. Therefore, Siann teaches the license as described by applicant's definition (see also parag. 100-108). Siann does not explicitly teach use of activation code as a cryptographic signature. However, Siann teaches using cryptographic techniques, such as a license to verify authenticity. As a cryptographic signature is a

cryptographic verification technique, which was well-known and widely practiced at the time of invention, it would have been obvious to the one skilled in art to use cryptographic signatures for verification. The motivation was to use a standard, commonly known and well developed technique to perform digital verification); launching, when the execution rights are verified, content on the playback device in accordance with the execution rights (Siann's invention is about providing access control pending digital verification. It is the purpose of Sian's invention to perform the verification, and after the verification is complete, launch the verified programs).

7.2. As per claim 26, Siann is directed to the method as in claim 25, wherein the playback device includes at least one of rights-enforcing hardware, rights-enforcing software, further including: authenticating the fights information using the rights-enforcing hardware or rights- enforcing software (paragraphs 53 and 96 disclose use of software and hardware to perform operations); enforcing the rights information on the system using the rights enforcing hardware or rights enforcing software, in response to the text-based activation code (see response to claims 1 and 25).

7.3. As per claims 27, 28, and 29, Siann is directed to a method including steps of sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable by

a system including a secure processor and a playback device under control of that secure processor; authenticating that rights information at the secure processor in response to mandatory security software executed by the secure processor; and enforcing that rights information on the system in response to that text-based message (see response to claims 25, 1, 4 and 5).

7.4. As per claim 30, Siann is directed to the method as in claim 27, wherein the steps of sending a text-based message include steps of sending a first message from a hand-held device using an SMS technique to a license server; sending a second message from the license server to the hand-held device, the second message including human-readable characters; and entering those characters to an input element coupled to the secure processor (see response to claims 13 and 25).

7.5. As per claim 31, Siann is directed to the method as in claim 27, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message, the closed content distribution system including the mandatory security software (see claim 25) being responsive to a private key in a public-key cryptosystem (private and public key cryptosystems were well-known in the art at the time of invention, and therefore it would have been obvious to use security software responsive to public and/or private public key cryptosystem).

7.6. Limitations of claims 32-33 are substantially the same as claim 25, with additional limitations all disclosed by Siann as indicated in claims 1-4 above.

7.7. Limitations of claims 34 and 35 are substantially the same as claims 25, and 1 to 9, with the added limitation of using a token to identify and deliver the signature to the playback device. Use of tokens to deliver a signature or other forms of authentication/authorization credentials was well-known and widely practiced at the time of invention. Barring any unexpected results, use of tokens as a method to deliver authentication credentials would have been trivial to a person skilled in the art at the time of invention.

7.8. As per claims 36, Siann is directed to a method comprising providing, in a closed content distribution system, an SMS text message that includes license information (license information is included in access data, which is delivered as depicted in Fig. 1B and associated text. SMS delivery method is disclosed in paragraph 43), in a form that is small enough for a human to conveniently enter (SMS messages are short enough to conveniently enter), the closed content distribution system including a playback device and a secure processor (the Media player as indicated in Fig. 4 and the associated text, includes a device to play the media to the output device and a secure processor (item 480 performs cryptographic functions to authenticate and access control)), wherein the SMS message is sent via a communication link not including the playback device or secure processor (see response to claim 1), constructing, at the playback device,

license parameters including device ID, a content ID, and a rights code identified by the activation code (parag. 79); using at least part of the SMS text message as a signature to authenticate the constructed parameters of possible execution rights (Siann teaches media authentication and access control using signatures and credentials delivered via messages sent to the Media Player in, for example, paragraph 86. Siann also teaches using SMS as a method of delivering messages (paragraph 43). Therefore, Siann teaches delivery of access control data in its methods of transmission, one of which is SMS. The access control parameters delivered via messages are used at the Media Player to enforce authentication and access control.); allowing content identified by the content ID to be executed or presented by the playback device or the secure processor, or by both in combination or conjunction in accordance with the constructed and authenticated license parameters, wherein the playback device or secure processor or both in combination or conjunction are associated with the device ID (see parag. 92 where device ID is identified for paying revenue to the owner, therefore teaching verification of the device ID as part of the verification and enforcing access rules); ensuring that rights information associated with the rights code is enforced by the playback device or the secure processor, or by both in combination or conjunction (see responses to claims 1 to 9).

7.9. Claims 37 and 38 are disclosed by Siann as it discloses claim 36 (see above) and all other limitations as described in responses to claims 1 to 21.

7.10. As per claims 39, Siann is directed to a method as in claim 36, including steps of encoding the license information using a digital signature, secure hash, or shared secret; and authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret (paragraph 51 discloses use of cryptography in securing different processes and digital signatures, hashes and shared secret are well-known methods of providing security using cryptographic methods).

7.11. As per claims 40 to 42, 44 to 46, 48 to 49 Siann's Fig. 1B and associated text discloses a method of delivery of content and all other limitations as described in responses to claims 1 to 21.

7.12. As per claim 43, Siann is directed to a method as in claim 36, wherein the communication link includes a cellular telephone (paragraph 41)

7.13. As per claims 47, Siann is directed to a method as in claim 36, wherein the secure processor includes a computing device capable of general purpose processing (paragraph 50).

7.14. As per claims 50, Siann is directed to a method as in claim 36, including steps of performing a commercial transaction concurrently with communication between a

license server and a user (paragraph 71 indicates that the user purchases content using the system, therefore performing a commercial transaction).

7.15. As per claims 51 to 65 Siann is directed to a method as in claim 50 and all other limitations as described in responses to claims 1 to 21.

7.16. As per claim 69 Siann is directed to a system comprising a closed content distribution system (Fig. 1B) including a playback device (fig. 3 item 310) and a secure processor (fig. 4 item 480); a communication link not including the playback device or secure processor (Fig. 1B item 162); a license server capable of being coupled to the communication link (Fig. 1B item 160); wherein the playback device or the secure processor, or both in combination or conjunction, includes mandatory security software that is configured to construct parameters of execution rights, and to use at least part of the text message as a signature to authenticate the constructed parameters of execution rights (paragraphs 53 and 96, and see response to claim 36).

7.17. As per claims 70 to 84, 86, 87, 89 to 90 Siann is directed to a method as in claim 69 and all other limitations as described in responses to claims 1 to 26.

7.18. As per claim 91, Siann is directed to the method of claim 1, further comprising: constructing parameters of execution rights (see response to claim 1) sending a text-based message to a hand-held device using an SMS technique (paragraph 43, also note that per paragraph 37, the Media Player is a portable, and therefore a hand-held,

device), the text-based message including information from which rights information is derivable by a system including a playback device (Fig. 1B and paragraph 43); and enforcing that rights information on the system in response to that text-based message (paragraph 80 and 39); wherein the steps of sending include a transport technique not including the playback device (Fig. 1B clearly indicates a transmission path separate from the media player, as described in paragraph 99), and the security is enforced by a mandatory hardware device (Fig. 4 and associated text), and using the message as a signature to authenticate the rights (Siann teaches cryptographic methods of verification and using digital signatures is a well-known method of authenticity verification).

7.19. As per claims 92 and 94, Siann teaches using cryptographic keys for verification, and public and secret (private) key cryptography is a well-known method of verification using keys, as explained in claim 31 above.

7.20 As per claim 93, Siann teaches using cryptographic verification as shown in claim 25 above. Note that MAC is a method of verification using cryptograph public or private keys, which was well-known in the art at the time of invention. Therefore, it would have been obvious to use MAC for verification, as explained in claim 31 above.

7.21. Limitations of claims 95-97 is substantially the same as portions of claims 1-21, and 25-27, and 92-94 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr
Examiner
Art Unit: 2139

Application/Control Number: 10/727,332

Page 20

Art Unit: 2139

/Kristine Kincaid/

Supervisory Patent Examiner, Art Unit 2139